

What in the heck are PORTS and how does it effect my firewall? On second thought, what's a FIREWALL?

A firewall is a term or name given for a service that regulates inbound and outbound network traffic. For example, Internet access can be given to Jane while Paul can be blocked from gaining access to the Internet. By the same token, incoming traffic can be granted or taken away as well. Blocking incoming traffic is how the firewall protects the personal computer (PC) on the network from hackers.

Now, in order to allow access to an internal PC by authorized people, the firewall will need to be opened. This is where PORTS come in.

There are around 9,999 ports that make up the firewall. Think of it as a big brick wall. To pass information through the wall you will need to make a hole in it. This is called opening a port. We open individual ports rather than the whole fire wall to maintain some level of security from hackers.

Now within the firewalls software, we can tell the firewall what port to open and to which PC to send the information to.

For example, and Internet browser uses port 80 to communicate with web servers like the one you are viewing right now. If port 80 were closed on my firewall, you would not be reading this wonderful FREE education. Your request for www.4maxvideo.com would have been blocked by my firewall. For me to allow others to access my web server I had to open port 80. Other examples of common ports would be FTP- port 21, Telnet port 23 and port 5631 for PCanywhere.

My philosophy:

Block all incoming traffic. Open only the ports that are needed.

Steve Detro 2006